Development of authentication code for multi-access optical code division multiplexing based quantum key distribution

ABSTRACT

One-weight authentication code for multi-user quantum key distribution (QKD) is proposed. The code is developed for Optical Code Division Multiplexing (OCDMA) based QKD network. A unique address assigned to individual user, coupled with degrading probability of predicting the source of the qubit transmitted in the channel offer excellent secure mechanism against any form of channel attack on OCDMA based QKD network. Flexibility in design as well as ease of modifying the number of users are equally exceptional quality presented by the code in contrast to Optical Orthogonal Code (OOC) earlier implemented for the same purpose. The code was successfully applied to eight simultaneous users at effective key rate of 32 bps over 27 km transmission distance.

Keyword: Authentications; Key distribution; Information security; Quantum communication; Cryptography